IN THE UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF MARYLAND

Southern Division

IN THE MATTER OF THE SEARCH OF:	)
	)
1. THE RESIDENCE PREMISES AT 4510 WOODLARK PLACE ROCKVILLE, MARYLAND	) 12-594 JKS
	)
2. A 1982 FORD F-150 TRUCK BEARING MARYLAND LICENSE PLATE IDENTIFIER 740598 AND VEHICLE IDENTIFICATION NUMBER 1FTDF15E2CNA50383	) 12-596 JKS
	)
3. A 1991 TOYOTA COROLLA AUTOMOBILE BEARING MARYLAND LICENSE PLATE IDENTIFIER JEX559 AND VEHICLE IDENTIFICATION NUMBER 1NXAE94A7MZ211123	) 12-597 JKS

AFFIDAVIT IN SUPPORT OF APPLICATION FOR THREE SEARCH WARRANTS

I, Thomas M. Shea, being duly sworn, state the following:

I. INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) assigned to the FBI's Washington Field Office in the District of Columbia. I am assigned to a Counterintelligence Squad which investigates crimes involving national security. I entered on duty as an FBI SA in July 2006. I have completed FBI training in the proper handling of classified information, and have been involved in the execution of search warrants and seizing evidence from residences and other locations. Prior to joining the FBI, I served as an Officer in the United States Marine Corps for approximately eight years.

2. This affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure in support of a warrant to search the residence premises located at 4510 Woodlark Place, Rockville, Maryland (hereinafter referred to as PREMISES), within the District of Maryland. This premises is occupied by Robert F. Harwin, who is the target of the investigation described in this affidavit. Further, warrants are requested to search two vehicles possessed at this premises by Robert F. Harwin. The premises and vehicles are further described in Attachment A.

3. Based upon information obtained by me, including information relayed to me by other SAs, and other sources to this investigation, there is probable cause to believe evidence, instrumentalities, and fruits of a violation of the TARGET OFFENSE (described in paragraph 4 below) may be located at the PREMISES and in HARWIN's vehicles, a 1982 Ford with Maryland License plate 740598 (FORD) and a 1991 Toyota with Maryland License plate JEX559 (TOYOTA). According to the Maryland Motor Vehicle Administration (MVA), the FORD and TOYOTA are registered to HARWIN at the PREMISES.

4. Based on the facts set forth below, I believe there is probable cause to believe that Robert F. Harwin committed the crime of Unauthorized Removal and Retention of Classified Documents or Material, in violation of 18 U.S.C. § 1924. Section 1924 provides in pertinent part:

> Whoever, being an officer, employee, contractor, or consultant of the United States, and, by virtue of his office, employment, position, or contract, becomes possessed of documents or materials containing classified information of the United States, knowingly removes such documents or materials without authority and with the intent to retain such documents or materials at an unauthorized location shall be fined under this title or imprisoned for not more than one year, or both.

Section 1924 further provides that the term "classified information of the United States" means "information originated, owned, or possessed by the United States Government concerning the

national defense or foreign relations of the United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security." Executive Order 13526, incorporating Executive Order 12958, and its successor orders states: that information is classified as "SECRET" if its unauthorized disclosure reasonably could be expected to cause serious damage to the national security; and that information is classified as "TOP SECRET" if its unauthorized disclosure reasonably could be expected to cause exceptionally grave damage to the national security. This offense is hereinafter referred to as the "TARGET OFFENSE."

5. The evidence, fruits, and instrumentalities of the TARGET OFFENSE consist of the items listed in Attachment B to the proposed Search Warrant (which is attached to this Affidavit).

6. I make this affidavit based upon information and evidence provided by witness statements, discussions, and reports submitted by other FBI employees, law enforcement officers, and other government agencies, as well as my own personal knowledge, training, and experience. Because this affidavit is being submitted in support of a search warrant, I have not included each and every fact known to me concerning this investigation. Further, the dates on which the incidents described herein occurred on or about the dates stated in this affidavit.

II. SUMMARY OF PROBABLE CAUSE

7. There is probable cause to believe Harwin is suspected of unlawfully removing classified information from his US government workplace in both paper and electronic form on numerous occasions over at least the past two months and unlawfully storing that classified information in his automobiles and at his residence. Not only did co-workers observe unusual behavior consistent with this allegation, as detailed below, but Harwin himself has made admissions to others, including investigators, that he has mishandled classified information.

Finally, investigators observed classified information and other US government computer media in Harwin's possession, that investigators believe he unlawfully removed from a US government facility. The following facts establish probable cause to believe that evidence of the alleged crime exists at the places to be searched and on or in the items to be seized.

III. BACKGROUND

8. Robert F. HARWIN is an Analyst employed by the National Geospatial Intelligence Agency (NGA) in Springfield, Virginia. In connection with his work for the NGA, HARWIN was granted a Top Secret (TS) security clearance.

9. According to NGA, HARWIN signed a Standard Form 312 "Classified Information Nondisclosure Agreement" and in doing so acknowledged, among other things, the following:

> (1) Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1, 1.2, 1.3, and 1.4(e) of Executive Order 12958, or any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government. (2) I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures. (3) I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency

(hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I disclose it, except to a person as provided in (a) or (b) above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information. (4) I have been advised that any breach of this Agreement may result I the termination of any such security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, *952 and 1924, Title 18, United States Code, *the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation. (5) I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may have come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

IV. FACTS SUPPORTING PROBABLE CAUSE

10. On December 14, 2011, an NGA co-worker of HARWIN was interviewed by officers from the NGA Counterintelligence Threat Mitigation Center. The co-worker (CW1) shared a workspace with HARWIN and had observed behavior which included carrying a heavy plastic bag out of NGA facilities at 0800-0900 hours on three to four different occasions.

11. Another co-worker (CW2) of HARWIN at the NGA reported HARWIN having numerous classified and unclassified documents on his desk which was unexplainable considering HARWIN's workload. Recently, while a pending polygraph examination was being discussed among employees, HARWIN stated to CW2 that he had accidentally taken classified documents to the PREMISES on several occasions but always brought the documents back the next day.

12. Pursuant to the interviews of the co-workers, the NGA began an investigation concerning HARWIN's possible unauthorized removal and retention of classified material. Pursuant to the NGA investigation, on January 20, 2012, a consent search for classified material was conducted of HARWIN's TOYOTA by NGA Police. Several documents were recovered during the search with SECRET and TOP SECRET markings. These documents discovered by the NGA police were, in fact, classified. Additionally, Computer Discs labeled with government markings were discovered within HARWIN's TOYOTA. An NGA official recognized one of the words on a disc as being possibly associated with a classified program.

13. During an interview with the FBI on January 20, 2012, HARWIN indicated he was unsure if classified information was present at the PREMISES. During this interview with the FBI, HARWIN initially stated there was no classified material located on the PREMISES. The FBI asked HARWIN, since he had initially said there was no classified material located in his car, but a consensual search later revealed that there was, whether it might be possible that classified material be located on the PREMISES. HARWIN indicated that he would like to tell the FBI that there was not any classified on the PREMISES, but he could not make any assurances. HARWIN also described himself as a hoarder. I know that *Hoarding* is the excessive collection of particular items, along with the inability to discard the items.

14. FBI Special Agents have maintained surveillance on Harwin and his residence since the evening of January 20, 2012. After classified information had been discovered in HARWIN's TOYOTA, and after HARWIN participated in a voluntary interview with the FBI pertaining to his handling of classified information, HARWIN was observed moving a bag from the PREMISES to the backseat of the TOYOTA. This occurred during the evening hours of January 20, 2012.

15. Since classified information was previously discovered in HARWIN's TOYOTA and since HARWIN recently professed to have taken classified information to his PREMISES, I have reason to believe that HARWIN has unlawfully retained classified information in the PREMISES and his automobiles.

16. Finally, based on HARWIN's mishandling of classified material found in his TOYOTA, I believe data contained on the Computer Discs found within the TOYOTA, displaying what are believed to be government markings, could contain evidence, instrumentalities, and fruits of a violation of the TARGET OFFENSE. Therefore, additional Computer Media potentially containing classified material could be found at the PREMISES and within HARWIN's automobiles.

V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

17. As described above and in Attachment B, this application seeks permission to search for classified information that might be found on the PREMISES and in HARWIN's TOYOTA and FORD, in whatever form it is found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all pursuant to Rule 41(e)(2)(B) of the Federal Rules of

Criminal Procedure.

(a) *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

1. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file do not actually disappear; rather, those data remain on the storage medium until it is overwritten by new data.

2. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

3. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

4. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

(b) *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the TARGET OFFENSE, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

1. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

2. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

3. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

4. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed

along to investigators. Whether data stored on a computer are evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

5. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

6. I know that at least the Computer Media could be an instrumentality of the TARGET OFFENSE, namely the CDs labeled with what are believed to be government markings discovered in HARWIN's TOYOTA. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that are evidence of how the computer was used; data that were sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

(c) *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of the premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises,

it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

1. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

2. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required

to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

3. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

(d) *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. Due to the level of classified material suspected to be contained on the electronic media, the FBI must review such material in an approved and accredited United States Government facility for the same level of classification. Accordingly, all of the suspected electronic media will be seized and not reviewed on-site.

VII. CONCLUSION

18. Based on all of the above facts, as well as my training and experience, I have probable cause to believe that Robert F. HARWIN has violated 18 U.S.C. Section 1924 and that contraband, evidence, instrumentalities and fruits of these violations may exist in the PREMISES

and in HARWIN's automobiles.

19. Accordingly, I respectfully request that the Court issue warrants authorizing the U.S. Government to search the residence of Robert F. HARWIN located at 4510 Woodlark Place Rockville, Maryland, within the District of Maryland, and HARWIN's vehicles, a 1991 Toyota with Maryland license plate number JEX559, and a 1982 Ford with Maryland license plate number 740598, wherever they may be located.

Thomas M. Shea
Special Agent
Federal Bureau of Investigation

~~SUBSCRIBED TO AND~~ SWORN before me this 22nd day of January, 2012. Subscribed before me 1/23/12

JILLYN SCHULZE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PLACES TO BE SEARCHED:

1. THE RESIDENCE PREMISES located at 4510 Woodlark Place, Rockville, Maryland, is a red, two floor, L-shaped, single family residential home and any outbuilding located on the property;

2. One Harwin vehicle is a light colored 1982 Ford F150 bearing Maryland License plate 740598 and VIN#1FTDF15E2CNA50383;

3. Another Harwin vehicle is a light colored 1991 Toyota Corolla bearing Maryland License plate JEX559 and VIN#1NXAE94A7MZ211123.

4. According to the Maryland Motor Vehicle Administration (MVA), the aforementioned vehicles are registered to Robert F. Harwin at THE RESIDENCE PREMISES.

ATTACHMENT B

ITEMS TO BE SEIZED:

Classified Documents or Materials

Any Documents, materials, electronic media, or any items of any sort containing classified information and/or classified national defense information as described in Executive Order 12958, maintained in any form, including electronic media maintained on computer devices.

Computer Terms And Procedures

a. As used above, the terms, records, documents, programs, applications or materials include records, documents, programs, applications or materials created, modified or stored in any form.

b. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices (collectively the "computer devices") to determine whether the computer devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data contained on the computer devices.

ii. If the computer devices can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, they will be searched on-site, and a computer device will be seized only if the search reveals it to contain any data that falls within the list of items to be seized set forth herein.

iii. If the computer devices cannot be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data, then the computer devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iv. In searching the computer devices, the computer personnel may examine all of the data contained in the computer devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

v. If the computer personnel seize the computer devices pursuant to subparagraph iii above, the computer personnel will initially search the computer devices within a reasonable amount of time not to exceed 90 days from the date of execution of the warrant. If, after conducting such an initial search, the case agents determine that a computer device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the computer device for further analysis; otherwise, the government will return the computer device.

If the government needs additional time to determine whether a computer device is an item to be seized or contains any data falling within the list of items to be seized pursuant to this warrant it may seek an extension of the time period from the Court within the original ninety day period from the date of execution of the warrant.

c. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones, and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices

or software.

v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

Re: Fw: AP and SW
Eisenberg, Harvey (USAMD)
to:
'Judge_Schulze@mdd.uscourts.gov'
01/22/2012 08:28 AM
Show Details

Thank you, Your Honor. Please enjoy the rest of your day knowing that you'll not be hearing from me again.....hopefully.
Respectfully,

Harvey Eisenberg
Assistant U.S. Attorney
Chief, National Security Section
District of Maryland

Coordinator, Anti-Terrorism
Advisory Council of Maryland
410.209.4843 (o)
443.677.1333 (m)

From: Judge_Schulze@mdd.uscourts.gov [mailto:Judge_Schulze@mdd.uscourts.gov]
Sent: Sunday, January 22, 2012 08:19 AM
To: Eisenberg, Harvey (USAMD)
Subject: Re: Fw: AP and SW

Mr. Eisenberg,
Agent Shea having affirmed that his affidavit is true and correct to the best of his knowledge, and upon my finding that probable cause exists, I hereby issue the warrants you have requested to search the premises at 4510 Woodlark Pl., Rockville, Md., the 1982 Ford Pickup, and the 1991 Toyota Corolla, all as further described in the affidavit.
The warrants issue on January 22, 2012 at 8:15 a.m. Documents to be executed on January 23, 2012, at the US Courthouse in Greenbelt.

Jillyn K. Schulze
United States Magistrate Judge
-----"Eisenberg, Harvey (USAMD)" <Harvey.Eisenberg@usdoj.gov> wrote: -----

> To: "'judge_schulze@mdd.uscourts.gov'" <judge_schulze@mdd.uscourts.gov>
> From: "Eisenberg, Harvey (USAMD)" <Harvey.Eisenberg@usdoj.gov>
> Date: 01/21/2012 07:15PM
> Subject: Fw: AP and SW
>
> Your Honor,
> Here are the Applications and proposed Warrants. Again, thank you.
> Respectfully,
>
> Harvey Eisenberg
> Assistant U.S. Attorney

Chief, National Security Section
District of Maryland

Coordinator, Anti-Terrorism
Advisory Council of Maryland
410.209.4843 (o)
443.677.1333 (m)

From: Condon, Michael J. [mailto:Michael.Condon@ic.fbi.gov]
Sent: Saturday, January 21, 2012 06:28 PM
To: Eisenberg, Harvey (USAMD); hee4812@verizon.net <hee4812@verizon.net>
Cc: Shea, Thomas M. (FBI)
Subject: AP and SW

[attachment "PREMISES AP.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]
[attachment "PREMISES SW.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]
[attachment "TOYOTA AP.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]
[attachment "TOYOTA SW.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]
[attachment "FORD AP.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]
[attachment "FORD SW.tif" removed by Judge Jillyn Schulze/MDD/04/USCOURTS]